This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method for on-line mass distribution of data products to end users, the method comprising:

maintaining an encrypted first portion of each of said data products at a first location;

maintaining an unencrypted second portion of each of said data products at a second location, wherein said second location is different from said first location;

for each of said end users, confirming the end user's entitlement to one of said data products;

obtaining an unencrypted second portion of said one of said data products from said second location;

after said step of confirming, obtaining an encrypted first portion of said one of said data products at said second location from said first location, obtaining a decryption key and using said decryption key to decrypt said encrypted first portion;

combining said decrypted first portion of said one of said data products and said unencrypted second portion of said one of said data products to form a combined product, wherein said step of combining is performed at said second location, wherein said end user is located at said second location;

storing said combined product on a portable computer-readable storage medium; and

providing said computer-readable storage medium having said combined first portion and second portion to said user, wherein the first portion of said data product comprises critical data that enables a program executed on a computing platform to use said data product including both the first portion and the second portion together for an intended purpose, wherein said user accesses said combined product from said storage medium with said computer platform at a third location different from said first location and said second location.

Claim 2 (original): The method of claim 1, wherein said data products include geographic databases.

Claim 3 (original): The method of claim 1, wherein said data products include digital copies of movies.

Claim 4 (original): The method of claim 1, wherein said data products include digital copies of musical songs.

Claim 5 (canceled).

Claim 6 (original): The method of claim 1, further comprising the step of:

prior to the step of combining, encrypting said first portion of one of said data products.

Claim 7 (canceled).

Claim 8 (currently amended): A system for secure on-line mass distribution of data products to end users comprising:

an authorization server at a first location having associated therewith copies of first portions of a plurality of data products, wherein said first portions of the data products do not include information to enable encrypted data to be decrypted;

a plurality of data distribution terminals at a plurality of locations different from said first location, each of said data distribution terminals has stored thereon copies of second portions of said plurality of data products;

a communications system that provides for exchange of data between said authorization server and said plurality of data distribution terminals, ~~and~~

a data distribution program that provides copies of said data products to those end users who are entitled to have said copies thereof, wherein said data distribution program provides a combined copy of a data product by combining a copy of the first portion of said data product obtained from said authorization server with a copy of the second portion of said data product obtained from one of said plurality of data distribution terminals, wherein said step of combining is performed at a location of said one of said plurality of data distribution terminals and said end user is located at said location of said one of said plurality of data distribution terminals; and

a storage device interface associated with said data distribution terminal, wherein said storage device interface stores said combined product on a portable computer-readable storage medium, wherein said user accesses said combined product from said storage medium with a computer platform at a location different from said location of said data distribution terminal.

Claim 9 (original): The system of claim 8, wherein said authorization server also has associated therewith an authorization database containing data indicating entitlement by said end users to copies of said data products.

Claim 10 (currently amended): A system for securely conveying a data product, the system comprising, in combination:

a first entity maintaining the first portion of the data product at a first location;

a second entity maintaining the second portion of the data product at a second location different from said first location;

a first set of logic executable by the first entity to encrypt the first portion so as to produce an encrypted first portion that can be decrypted using a first decryption key, wherein the first entity sends the encrypted first portion via a telecommunications link to the second entity; and

a second set of logic executable by the second entity, upon receipt of the encrypted first portion, to record onto a storage medium the encrypted first portion and the unencrypted second portion, wherein an end user of the data product is located at said second location where the encrypted first portion and the unencrypted second portion are recorded onto the storage medium;

wherein the storage medium may be provided to a third entity, which, if provided with access to the first decryption key, can in turn access the data product, wherein the first portion of said data product comprises critical data that enables a program executed on a computing platform to use said data product including both the first portion and the second portion together for an intended purpose, wherein said user accesses said data product at a location different from said first location and said second location.

Claim 11 (original): The system of claim 10, wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product, and wherein the second set of logic is further executable to record onto the storage medium the encrypted authorization key.

Claim 12 (original): The system of claim 11, wherein the second decryption key is derived as a function of an environmental parameter.

Claim 13 (original): The system of claim 12, wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product.

Claim 14 (original): The system of claim 11, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization key, to thereby gain access to the verification information, and to use the verification information to validate use of the data product.

Claim 15 (original): The system of claim 11, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization information, to thereby gain access to the verification information, and to compare at least a portion of the verification information to predetermined information associated with the third entity so as to determine whether the third entity is authorized to access the data product.

Claim 16 (original): The system of claim 15, wherein the predetermined information associated with the third entity comprises an identification code.

Claim 17 (original): The system of claim 10, wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product.

Claim 18 (original): The system of claim 17, wherein the second decryption key is derived as a function of an environmental parameter.

Claim 19 (original): The system of claim 18, wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product.

Claim 20 (original): The system of claim 17, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization key, to thereby gain access to the verification information, and to use the verification information to validate storage of the data product.

Claim 21 (original): The system of claim 17, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization information, to thereby gain access to the verification information, and to compare at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to store the data product.

Claim 22 (original): The system of claim 21, wherein the predetermined information associated with the storage medium comprises an identification code.

Claim 23 (original): The system of claim 10, wherein the data product comprises geographic information and the third entity comprises a navigation system.

Claim 24 (currently amended): A method for securely conveying a data product, the method comprising, in combination:

at a first entity at a first location, maintaining a first portion of the data product and encrypting the first portion of the data product so as to produce an encrypted first portion that can be decrypted using a first decryption key;

sending the encrypted first portion via a telecommunications link from the first entity to a second entity at a second location;

receiving the encrypted first portion at the second entity, wherein an unencrypted second portion of the data product is maintained at said second entity;

at the second entity, recording onto a storage medium the encrypted first portion and the second portion wherein an end user of the data product is located at said second location where the encrypted first portion and the second portion are recorded onto the storage medium; and

thereafter providing the storage medium to a third entity, whereby, if the third entity has access to the first decryption key, the third entity may decrypt the encrypted first portion and thereby gain access to the data product, wherein said third entity is at a location different from said first location and said second location.

Claim 25 (original): The method of claim 24, further comprising sending to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product.

Claim 26 (original): The method of claim 25, further comprising generating the second decryption key as a function of an environmental parameter.

Claim 27 (original): The method of claim 26, wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product.

Claim 28 (original): The method of claim 27, further comprising:

the third entity generating the second decryption key as the function of the identification code;

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate storage of the data product.

Claim 29 (original): The method of claim 25, further comprising:

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate use of the data product.

Claim 30 (original): The method of claim 29, wherein using the verification information to validate use of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the third entity so as to determine whether the third entity is authorized to access the data product.

Claim 31 (original): The method of claim 30, wherein the predetermined information associated with the third entity comprises an identification code.

Claim 32 (original): The method of claim 24, further comprising sending to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product.

Claim 33 (original): The method of claim 32, further comprising generating the second decryption key as a function of an environmental parameter.

Claim 34 (original): The method of claim 33, wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product.

Claim 35 (original): The method of claim 34, further comprising:

the third entity generating the second decryption key as the function of the identification code;

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate storage of the data product.

Claim 36 (original): The method of claim 32, further comprising:

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate storage of the data product.

Claim 37 (original): The method of claim 36, wherein using the verification information to validate storage of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to store the data product.

Claim 38 (original): The method of claim 37, wherein the predetermined information associated with the storage medium comprises an identification code.

Claim 39 (original): The method of claim 24, wherein the data product comprises geographic information and the third entity comprises a navigation system.